

# COUNTING ALGEBRAIC INTEGERS OF FIXED DEGREE AND BOUNDED HEIGHT

FABRIZIO BARROERO

ABSTRACT. Let  $k$  be a number field. For  $\mathcal{H} \rightarrow \infty$ , we give an asymptotic formula for the number of algebraic integers of absolute Weil height bounded by  $\mathcal{H}$  and fixed degree over  $k$ .

## 1. INTRODUCTION

Let  $k$  be a number field of degree  $m$  over  $\mathbb{Q}$ . We count the number of algebraic integers  $\beta$  of degree  $e$  over  $k$  and bounded height. Here and in the rest of the article, by height we mean the non-logarithmic absolute Weil height  $H$  on the affine space  $\overline{\mathbb{Q}}^n$  (see [3], p. 16).

For positive rational integers  $n$  and  $e$ , and a fixed algebraic closure  $\overline{k}$  of  $k$ , let

$$k(n, e) = \{\beta \in \overline{k}^n : [k(\beta) : k] = e\},$$

where  $k(\beta)$  is the field obtained by adjoining all the coordinates of  $\beta$  to  $k$ . By Northcott's Theorem [12] any subset of  $k(n, e)$  of uniformly bounded height is finite. Therefore, for any subset  $S$  of  $k(n, e)$  and  $\mathcal{H} > 0$ , we may introduce the following counting function

$$N(S, \mathcal{H}) = |\{\beta \in S : H(\beta) \leq \mathcal{H}\}|.$$

The counting function  $N(k(n, e), \mathcal{H})$  has been investigated by various people. The best known and one of the earliest is a result of Schanuel [15] who gave an asymptotic formula for  $N(k(n, 1), \mathcal{H})$ . The first who dropped the restriction of the coordinates to lie in a fix number field was Schmidt. In [16], he found upper and lower bounds for  $N(k(n, e), \mathcal{H})$  and in [17] he gave an asymptotic formula for  $N(\mathbb{Q}(n, 2), \mathcal{H})$ . Shortly afterwards, Gao [7] found the asymptotics for  $N(\mathbb{Q}(n, e), \mathcal{H})$ , provided  $n > e$ . Later Masser and Vaaler [10] established an asymptotic estimate for  $N(k(1, e), \mathcal{H})$ . Finally, Widmer [19] proved an asymptotic formula for  $N(k(n, e), \mathcal{H})$  for arbitrary number fields  $k$ , provided  $n > 5e/2 + 5 + 2/me$ . However, for general  $n$  and  $e$  even the correct order of magnitude for  $N(k(n, e), \mathcal{H})$  remains unknown.

In this article we are interested in counting integral points, i.e., points  $\beta \in \overline{k}^n$ , whose coordinates are algebraic integers. Let  $\mathcal{O}_k$  and  $\mathcal{O}_{\overline{k}}$  be, respectively, the ring of algebraic integers in  $k$  and  $\overline{k}$ . We introduce

$$\mathcal{O}_k(n, e) = k(n, e) \cap \mathcal{O}_{\overline{k}}^n = \{\beta \in \mathcal{O}_{\overline{k}}^n : [k(\beta) : k] = e\}.$$

---

*Date:* May 9, 2013.

2010 *Mathematics Subject Classification.* Primary 11G50, 11R04.

F. Barroero is supported by the Austrian Science Foundation (FWF) project W1230-N13.

Possibly, the first asymptotic result (besides the trivial cases  $\mathcal{O}_{\mathbb{Q}}(n, 1) = \mathbb{Z}^n$ ) can be found in Lang's book [8]. Lang states, without proof,

$$N(\mathcal{O}_k(1, 1), \mathcal{H}) = \gamma_k \mathcal{H}^m (\log \mathcal{H})^q + O\left(\mathcal{H}^m (\log \mathcal{H})^{q-1}\right),$$

where  $m = [k : \mathbb{Q}]$ ,  $q$  is the rank of the unit group of the ring of integers  $\mathcal{O}_k$ , and  $\gamma_k$  is an unspecified positive constant, depending on  $k$ . More recently, Widmer [18] established the following asymptotic formula

$$(1.1) \quad N(\mathcal{O}_k(n, e), \mathcal{H}) = \sum_{i=0}^t D_i \mathcal{H}^{men} (\log \mathcal{H}^{me})^i + O(\mathcal{H}^{men-1} (\log \mathcal{H})^t),$$

provided  $e = 1$  or  $n > e + C_{n,e}$ , for some explicit  $C_{n,e} \leq 7$ . Here  $t = e(q+1) - 1$ , and the constants  $D_i = D_i(k, n, e)$  are explicitly given. Widmer's result is fairly specific in the sense that he works only with the absolute non-logarithmic Weil height  $H$ . On the other hands the methods used in [18] are quite general and powerful, and certainly can be applied to handle other heights (such as the heights used by Masser and Vaaler in [10] to deduce their main result). As mentioned in [18] this might lead to multiterm expansions as in (1.1) for  $N(\mathcal{O}_k(1, e), \mathcal{H})$ .

However, for the moment, such generalizations of (1.1) are not available, and thus the work [18] of Widmer does not provide any results in the case  $n = 1$  and  $e > 1$ .

But Chern and Vaaler in [5], proved an asymptotic formula for the number of monic polynomials in  $\mathbb{Z}[x]$  of given degree and bounded Mahler measure. Theorem 6 of [5] immediately implies the following result

$$(1.2) \quad N(\mathcal{O}_{\mathbb{Q}}(1, e), \mathcal{H}) = C_e \mathcal{H}^{e^2} + O\left(\mathcal{H}^{e^2-1}\right),$$

for some explicitly given positive real constant  $C_e$ . Theorem 1.1 extends Chern and Vaaler's result to arbitrary ground fields  $k$ .

For positive rational integers  $e$  we define

$$C_{\mathbb{R},e} = 2^{e-M} \left( \prod_{l=1}^M \left( \frac{2l}{2l+1} \right)^{e-2l} \right) \frac{e^M}{M!},$$

with  $M = \lfloor \frac{e-1}{2} \rfloor$ , and

$$C_{\mathbb{C},e} = \pi^e \frac{e^e}{(e!)^2}.$$

And, finally, let

$$(1.3) \quad C_k^{(e)} = \frac{e^{2q+1} 2^{se} m^q}{q! \left( \sqrt{|\Delta_k|} \right)^e} C_{\mathbb{R},e}^r C_{\mathbb{C},e}^s,$$

where  $m = [k : \mathbb{Q}]$ ,  $r$  is the number of real embeddings of  $k$ ,  $s$  the number of pairs of complex conjugate embeddings,  $q = r + s - 1$ , and  $\Delta_k$  denotes the discriminant of  $k$ .

For nonnegative real functions  $f(X), g(X), h(X)$  and  $X_0 \in \mathbb{R}$  we write  $f(X) = g(X) + O(h(X))$  as  $X \geq X_0$  tends to infinity if there is  $C_0$  such that  $|f(X) - g(X)| \leq C_0 h(X)$  for all  $X \geq X_0$ .

**Theorem 1.1.** *Let  $e$  be a positive integer, and let  $k$  be a number field. Then, as  $\mathcal{H} \geq 2$  tends to infinity, we have*

$$N(\mathcal{O}_k(1, e), \mathcal{H}) = C_k^{(e)} \mathcal{H}^{me^2} (\log \mathcal{H})^q + \begin{cases} O\left(\mathcal{H}^{me^2} (\log \mathcal{H})^{q-1}\right), & \text{if } q \geq 1, \\ O\left(\mathcal{H}^{e(me-1)} \mathcal{L}\right), & \text{if } q = 0, \end{cases}$$

where  $\mathcal{L} = \log \mathcal{H}$  if  $(m, e) = (1, 2)$  and 1 otherwise. The implicit constant in the error term depends only on  $m$  and  $e$ .

Let us mention two simple examples. The number of algebraic integers  $\alpha$  quadratic over  $\mathbb{Q}(\sqrt{2})$  with  $H(\alpha) \leq \mathcal{H}$  is

$$32\mathcal{H}^8 \log \mathcal{H} + O(\mathcal{H}^8).$$

In case  $e = 3$ , we have

$$108\sqrt{2}\mathcal{H}^{18} \log \mathcal{H} + O(\mathcal{H}^{18})$$

algebraic integers  $\alpha$  cubic over  $\mathbb{Q}(\sqrt{2})$  with  $H(\alpha) \leq \mathcal{H}$ .

Our proof relies on a new lattice counting theorem for definable sets in an o-minimal structure [1], which uses recent results in Model theory, such as Pila and Wilkie's refinement of the Reparametrization Lemma [13]. Indeed, our proof is fairly short, and more straightforward than the approach of [18], but to the expense that we do not get a multiterm expansion.

In [10], Masser and Vaaler observed that the limit for  $\mathcal{H} \rightarrow \infty$  of

$$\frac{N(k(1, e), \mathcal{H}^{\frac{1}{e}})}{N(k(e, 1), \mathcal{H})}$$

is a rational number. Moreover, they asked if this can be extended to some sort of reciprocity law, i.e., whether

$$\lim_{\mathcal{H} \rightarrow \infty} \frac{N(k(n, e), \mathcal{H}^{\frac{1}{e}})}{N(k(e, n), \mathcal{H}^{\frac{1}{n}})} \in \mathbb{Q}.$$

If we consider only the first term in (1.1), and combine it with Theorem 1.1 we see that

$$\lim_{\mathcal{H} \rightarrow \infty} \frac{N(\mathcal{O}_k(1, e), \mathcal{H}^{\frac{1}{e}})}{N(\mathcal{O}_k(e, 1), \mathcal{H})} = e^{q+1} \left( \frac{C_{\mathbb{R}, e}}{2^e} \right)^r \left( \frac{C_{\mathbb{C}, e}}{\pi^e} \right)^s$$

is a rational number depending only on  $e$ ,  $r$  and  $s$ . As Masser and Vaaler did, one can ask again whether

$$\lim_{\mathcal{H} \rightarrow \infty} \frac{N(\mathcal{O}_k(n, e), \mathcal{H}^{\frac{1}{e}})}{N(\mathcal{O}_k(e, n), \mathcal{H}^{\frac{1}{n}})} \in \mathbb{Q}.$$

## 2. COUNTING MONIC POLYNOMIALS

In this section we see how our problem translates to counting monic polynomials of fixed degree that assume a uniformly bounded value under a certain real valued function called  $M^k$ , defined using the Mahler measure.

Recall we fixed a number field  $k$  of degree  $m$  over  $\mathbb{Q}$  and  $\mathcal{O}_k$  is its ring of integers. Let  $\sigma_1, \dots, \sigma_r$  be the real embeddings of  $k$  and  $\sigma_{r+1}, \dots, \sigma_m$  be the strictly complex ones, indexed in such a way that  $\sigma_j = \bar{\sigma}_{j+s}$  for  $j = r+1, \dots, r+s$ . Therefore,  $r$  and  $s$  are, respectively, the number of real and pairs of conjugate complex embeddings of  $k$  and  $m = r+2s$ . We put  $d_i = 1$  for  $i = 1, \dots, r$  and  $d_i = 2$  for  $i = r+1, \dots, r+s$  and fix a positive integer  $e$ . Let us recall the definition of the Mahler measure.

**Definition 2.1.** If  $f = z_0X^d + z_1X^{d-1} + \dots + z_d \in \mathbb{C}[X]$  is a nonzero polynomial of degree  $d$  with roots  $\alpha_1, \dots, \alpha_d$ , the Mahler measure of  $f$  is defined to be

$$M(f) = |z_0| \prod_{i=1}^d \max\{1, |\alpha_i|\}.$$

Moreover, we set  $M(0) = 0$ .

We see  $M$  as a function  $\mathbb{C}[X] \rightarrow [0, \infty)$  and define

$$\begin{aligned} M^k : k[X] &\rightarrow [0, \infty) \\ f &\mapsto \prod_{i=1}^{r+s} M(\sigma_i(f))^{\frac{d_i}{m}}, \end{aligned}$$

where  $\sigma_i$  acts on the coefficients of  $f$ . Note that, for every  $\alpha \in \mathcal{O}_k$ ,

$$(2.1) \quad M^k(X - \alpha) = \prod_{i=1}^{r+s} \max\{1, |\sigma_i(\alpha)|\}^{\frac{d_i}{m}} = H(\alpha).$$

In fact, if  $\alpha \in \mathcal{O}_k$  then  $|\alpha|_v \leq 1$  for every non-archimedean place  $v$  of  $k$ .

Moreover, the Mahler measure is multiplicative by definition, i.e.,

$$M(fg) = M(f)M(g),$$

and one can see that

$$M^k(fg) = M^k(f)M^k(g),$$

for every  $f, g \in k[X]$ .

We define  $\mathcal{M}^k(e, \mathcal{H})$  to be the set of monic  $f \in \mathcal{O}_k[X]$  of degree  $e$  and  $M^k(f) \leq \mathcal{H}$ . It is easy to see that  $\mathcal{M}^k(e, \mathcal{H})$  is finite for all  $\mathcal{H}$ . The following theorem gives an estimate for its cardinality.

**Theorem 2.1.** For every  $\mathcal{H}_0 > 1$  there exists a  $D_0$  such that, for every  $\mathcal{H} \geq \mathcal{H}_0$ ,

$$(2.2) \quad \left| |\mathcal{M}^k(e, \mathcal{H})| - \frac{C_k^{(e)}}{e^{q+1}} \mathcal{H}^{me} (\log \mathcal{H})^q \right| \leq \begin{cases} D_0 \mathcal{H}^{me} (\log \mathcal{H})^{q-1}, & \text{if } q \geq 1, \\ D_0 \mathcal{H}^{me-1}, & \text{if } q = 0, \end{cases}$$

where  $q = r + s - 1$ . The constant  $D_0$  depends only on  $\mathcal{H}_0$ ,  $m$  and  $e$ .

Note that our constant  $C_k^{(e)}$  defined in (1.3), is bounded if we fix  $m$  and  $e$  and we let  $k$  vary among all number fields of degree  $m$ . This implies that there exists a real constants  $C^{(m,e)}$ , depending only on  $m$  and  $e$ , such that  $|\mathcal{M}^k(e, \mathcal{H})|$  is bounded from above by

$$(2.3) \quad C^{(m,e)} \mathcal{H}^{me} (\log \mathcal{H} + 1)^q,$$

for every  $\mathcal{H} \geq 1$ .

We prove Theorem 2.1 later and for the rest of this section we derive Theorem 1.1 from Theorem 2.1. We follow the line of Masser and Vaaler [10].

Now we want to restrict to monic  $f$  irreducible over  $k$ . Let  $\widetilde{\mathcal{M}}^k(e, \mathcal{H})$  be the set of polynomials in  $\mathcal{M}^k(e, \mathcal{H})$  that are irreducible over  $k$ .

**Corollary 2.2.** For every  $\mathcal{H}_0 > 1$  there exists a  $F_0$  such that, for every  $\mathcal{H} \geq \mathcal{H}_0$ ,

$$(2.4) \quad \left| |\widetilde{\mathcal{M}}^k(e, \mathcal{H})| - \frac{C_k^{(e)}}{e^{q+1}} \mathcal{H}^{me} (\log \mathcal{H})^q \right| \leq \begin{cases} F_0 \mathcal{H}^{me} (\log \mathcal{H})^{q-1}, & \text{if } q \geq 1, \\ F_0 \mathcal{H}^{me-1} \mathcal{L}, & \text{if } q = 0, \end{cases}$$

where  $\mathcal{L} = \log \mathcal{H}$  if  $(m, e) = (1, 2)$  and 1 otherwise. The constant  $F_0$  depends again only on  $\mathcal{H}_0$ ,  $m$  and  $e$ .

*Proof.* For  $e = 1$  there is nothing to prove. Suppose  $e > 1$ . We show that, up to a constant, the number of all monic reducible  $f \in \mathcal{O}_k[X]$  of degree  $e$  with  $M^k(f) \leq \mathcal{H}$  is not larger than the right hand side of (2.2), except for the case  $(m, e) = (1, 2)$ .

Consider all  $f = gh \in \mathcal{M}^k(e, \mathcal{H})$  with  $g, h \in \mathcal{O}_k[X]$  monic of degree  $a$  and  $b$  respectively, with  $0 < a \leq b < e$  and  $a + b = e$ . We have  $1 \leq M^k(g), M^k(h) \leq \mathcal{H}$  because  $g$  and  $h$  are monic. Thus, there exists a positive integer  $l$  such that  $2^{l-1} \leq M^k(g) < 2^l$ . Note that  $l$  must satisfy

$$(2.5) \quad 1 \leq l \leq \frac{\log \mathcal{H}}{\log 2} + 1 \leq 2 \log \mathcal{H} + 1.$$

Since  $M^k$  is multiplicative,

$$M^k(h) = \frac{M^k(f)}{M^k(g)} \leq 2^{1-l} \mathcal{H}.$$

Using (2.3) and noting that  $2^l \leq 2\mathcal{H}$ , we can say that there are at most

$$C^{(m,a)} (2^l)^{ma} (\log 2^l + 1)^q \leq C^{(m,a)} (2^l)^{ma} (\log \mathcal{H} + 2)^q$$

possibilities for  $g$  and

$$C^{(m,b)} (2^{1-l} \mathcal{H})^{mb} (\log (2^{1-l} \mathcal{H}) + 1)^q \leq C^{(m,b)} (2^{1-l} \mathcal{H})^{mb} (\log \mathcal{H} + 2)^q$$

possibilities for  $h$ . Therefore, we have at most

$$(2.6) \quad C' \mathcal{H}^{mb} 2^{ml(a-b)} (\log \mathcal{H} + 2)^{2q}$$

possibilities for  $gh$  with  $M^k(gh) \leq \mathcal{H}$  and  $2^{l-1} \leq M^k(g) < 2^l$ , where  $C'$  is a real constant. Since there are only finitely many choices for  $a$  and  $b$  we can take  $C'$  to depend only on  $m$  and  $e$ .

If  $a = b = \frac{e}{2}$  then (2.6) is

$$C' \mathcal{H}^{m\frac{e}{2}} (\log \mathcal{H} + 2)^{2q}.$$

Summing over all  $l$ ,  $1 \leq l \leq \lfloor 2 \log \mathcal{H} \rfloor + 1$  (recall (2.5)), gives an extra factor  $2 \log \mathcal{H} + 1$ . Therefore, when  $a = b$ , there are at most

$$C' \mathcal{H}^{\frac{me}{2}} (2 \log \mathcal{H} + 2)^{2q+1}$$

possibilities for  $f = gh$ , with  $M^k(f) \leq \mathcal{H}$ . If  $(m, e) \neq (1, 2)$ , this has smaller order than the right hand side of (2.2), since  $me > 2$  implies  $\frac{me}{2} < me - 1$ . In the case  $(m, e) = (1, 2)$  we get  $C' \mathcal{H} (2 \log \mathcal{H} + 2)$  and we need an additional logarithm factor.

In the case  $a < b$ , summing  $2^{ml(a-b)}$  over all  $l$ ,  $1 \leq l \leq \lfloor 2 \log \mathcal{H} \rfloor + 1 = L$ , we get

$$\sum_{l=1}^L \left( 2^{m(a-b)} \right)^l \leq \sum_{l=1}^L 2^{-l} \leq 1.$$

Thus, recalling  $b \leq e - 1$ , when  $a < b$ , there are at most

$$C'' \mathcal{H}^{m(e-1)} (\log \mathcal{H} + 2)^{2q}$$

possibilities for  $f = gh$ , with  $M^k(f) \leq \mathcal{H}$ , where again  $C''$  depends only on  $m$  and  $e$ . This is again not larger than the right hand side of (2.2).  $\square$

For the last step of the proof we link such monic irreducible polynomials with their roots.

**Lemma 2.3.** *An algebraic integer  $\beta$  has degree  $e$  over  $k$  and  $H(\beta) \leq \mathcal{H}$  if and only if it is a root of a monic irreducible polynomial  $f \in \mathcal{O}_k[X]$  of degree  $e$  with  $M^k(f) \leq \mathcal{H}^e$*

*Proof.* Suppose  $f \in \mathcal{O}_k[X]$  is a monic irreducible polynomial of degree  $e$  and  $\beta$  is one of its roots, i.e.,  $\beta$  is an algebraic integer with  $[k(\beta) : k] = e$  and minimal polynomial  $f$  over  $k$ . We claim that

$$M^k(f) = H(\beta)^e.$$

We first need to show that we can define an absolute  $M^{\overline{\mathbb{Q}}}$  over  $\overline{\mathbb{Q}}[X]$  that, restricted to any  $k[X]$ , equals  $M^k$ . Recall that  $[k : \mathbb{Q}] = m$ . Let  $k'$  be a finite extension of  $k$  with  $[k' : \mathbb{Q}] = m'$ . We put  $M_{k,\infty}$  for the set of infinite places of  $k$ . For every  $w \in M_{k,\infty}$ ,  $\sigma_w$  is the corresponding embedding into  $\mathbb{C}$  and  $d_w$  is the local degree, i.e.  $d_w = 1$  or  $2$  if  $w$  corresponds to a real or a strictly complex embedding, respectively. Recall (see [11], Ch.II, (8.4) Corollary)

$$\sum_{\substack{v \in M_{k',\infty} \\ v|w}} d_v = d_w[k' : k] = d_w \frac{m'}{m}.$$

For any  $f \in k[X]$ , we have

$$\begin{aligned} M^{k'}(f) &= \prod_{v \in M_{k',\infty}} M(\sigma_v(f))^{\frac{d_v}{m'}} = \prod_{w \in M_{k,\infty}} \prod_{\substack{v \in M_{k',\infty} \\ v|w}} M(\sigma_v(f))^{\frac{d_v}{m'}} = \\ &= \prod_{w \in M_{k,\infty}} M(\sigma_w(f))^{\sum_{v|w} \frac{d_v}{m'}} = \prod_{w \in M_{k,\infty}} M(\sigma_w(f))^{\frac{d_w}{m}} = M^k(f). \end{aligned}$$

Suppose  $f = (X - \alpha_1) \cdots (X - \alpha_e)$ . Since the  $\alpha_i$  are algebraic integers, by (2.1), we have

$$M^{\overline{\mathbb{Q}}}(X - \alpha_i) = M^{\mathbb{Q}(\alpha_i)}(X - \alpha_i) = H(\alpha_i),$$

and the  $\alpha_i$  have the same height because they are conjugate (see [3], Proposition 1.5.17). Moreover, by the multiplicativity of  $M^k$  we can see that

$$M^k(f) = M^{\overline{\mathbb{Q}}}(f) = \prod_{i=1}^e M^{\overline{\mathbb{Q}}}(X - \alpha_i) = H(\alpha_i)^e,$$

for any  $\alpha_j$  root of  $f$ . □

Lemma 2.3 implies that  $N(\mathcal{O}_k(1, e), \mathcal{H}) = e \left| \widetilde{\mathcal{M}}^k(e, \mathcal{H}^e) \right|$  because there are  $e$  different  $\beta$  with the same minimal polynomial  $f$  over  $k$ . Therefore, by (2.4), we have that for every  $\mathcal{H}_0 > 1$  there exists a  $C_0$ , depending only on  $\mathcal{H}_0$ ,  $m$  and  $e$ , such that for every  $\mathcal{H} \geq \mathcal{H}_0$ ,

$$\left| N(\mathcal{O}_k(1, e), \mathcal{H}) - C_k^{(e)} \mathcal{H}^{me^2} (\log \mathcal{H})^q \right| \leq \begin{cases} C_0 \mathcal{H}^{me^2} (\log \mathcal{H})^{q-1}, & \text{if } q \geq 1, \\ C_0 \mathcal{H}^{e(me-1)} \mathcal{L}, & \text{if } q = 0, \end{cases}$$

where  $\mathcal{L} = \log \mathcal{H}$  if  $(m, e) = (1, 2)$  and 1 otherwise. We get Theorem 1.1 by choosing  $\mathcal{H}_0 = 2$ .

## 3. A COUNTING PRINCIPLE

In this section we introduce the counting theorem that will be used to prove Theorem 2.1. The principle dates back to Davenport [6] and was developed by several authors. In a previous work [1] the author and Widmer formulated a counting theorem that relies on Davenport's result and uses o-minimal structures. The full generality of Theorem 1.3 of [1] is not needed here as we are going to count lattice points in semialgebraic sets.

**Definition 3.1.** *A semialgebraic subset of  $\mathbb{R}^n$  is a set of the form*

$$\bigcup_{i=1}^N \bigcap_{j=1}^{M_i} \{\mathbf{x} \in \mathbb{R}^n : f_{i,j}(\mathbf{x}) *_{i,j} 0\},$$

where  $f_{i,j} \in \mathbb{R}[X_1, \dots, X_n]$  and the  $*_{i,j}$  are either  $<$  or  $=$ .

A very important feature of semialgebraic sets is the fact that this collection of subsets of the Euclidean spaces is closed under projections. This is the well known Tarski-Seidenberg principle.

**Theorem 3.1** ([2], Theorem 1.5). *Let  $A \in \mathbb{R}^{n+1}$  be a semialgebraic set, then  $\pi(A) \in \mathbb{R}^n$  is semialgebraic, where  $\pi : \mathbb{R}^{n+1} \rightarrow \mathbb{R}^n$  is the projection map on the first  $n$  coordinates.*

Let  $S \subseteq \mathbb{R}^{n+n'}$ , for a  $\mathbf{t} \in \mathbb{R}^{n'}$  we call  $S_{\mathbf{t}} = \{\mathbf{x} \in \mathbb{R}^n : (\mathbf{x}, \mathbf{t}) \in S\}$  the fiber of  $S$  above  $\mathbf{t}$ . Clearly, if  $S$  is semialgebraic also the fibers  $S_{\mathbf{t}}$  are semialgebraic. If so, we call  $S$  a semialgebraic family.

Let  $\Lambda$  be a lattice of  $\mathbb{R}^n$ , i.e., the  $\mathbb{Z}$ -span of  $n$  linearly independent vectors of  $\mathbb{R}^n$ . Recall that  $\lambda_i = \lambda_i(\Lambda)$  for  $i = 1, \dots, n$  are the successive minima of  $\Lambda$  with respect to the zero centered unit ball  $B_0(1)$ , i.e., for  $i = 1, \dots, n$

$$\lambda_i = \inf\{\lambda : B_0(\lambda) \cap \Lambda \text{ contains } i \text{ linearly independent vectors}\}.$$

The following theorem is a special case of Theorem 1.3 of [1].

**Theorem 3.2.** *Let  $Z \subset \mathbb{R}^{n+n'}$  be a semialgebraic family and suppose the fibers  $Z_{\mathbf{t}}$  are bounded. Then there exists a constant  $c_Z \in \mathbb{R}$ , depending only on the family, such that, for every  $\mathbf{t} \in \mathbb{R}^{n'}$ ,*

$$\left| |Z_{\mathbf{t}} \cap \Lambda| - \frac{\text{Vol}(Z_{\mathbf{t}})}{\det \Lambda} \right| \leq \sum_{j=0}^{n-1} c_Z \frac{V_j(Z_{\mathbf{t}})}{\lambda_1 \cdots \lambda_j},$$

where  $V_j(Z_{\mathbf{t}})$  is the sum of the  $j$ -dimensional volumes of the orthogonal projections of  $Z_{\mathbf{t}}$  on every  $j$ -dimensional coordinate subspace of  $\mathbb{R}^n$  and  $V_0(Z_{\mathbf{t}}) = 1$ .

## 4. A SEMIALGEBRAIC FAMILY

In this section we introduce the family we want to apply Theorem 3.2 to.

We see the Mahler measure as a function of the coefficients of the polynomial. We fix  $n > 0$  and define  $M : \mathbb{R}^{n+1}$  or  $\mathbb{C}^{n+1} \rightarrow [0, \infty)$  such that

$$M(z_0, \dots, z_n) = M(z_0 X^n + \cdots + z_n),$$

for  $\mathbf{z} \in \mathbb{R}^{n+1}$  or  $\mathbb{C}^{n+1}$ . This two functions satisfy the definition of bounded distance function in the sense of the geometry of numbers, i.e.,

- (1)  $M$  is continuous;

- (2)  $M(\mathbf{z}) = 0$  if and only if  $\mathbf{z} = \mathbf{0}$ ;
- (3)  $M(w\mathbf{z}) = |w|M(\mathbf{z})$ , for any scalar  $w \in \mathbb{R}$  or  $\mathbb{C}$ .

Properties (2) and (3) are obvious from the definition, while continuity was proved already by Mahler (see [9], Lemma 1).

Let  $M_1$  be the monic Mahler measure function, i.e.,  $M_1(\mathbf{z}) = M(1, \mathbf{z})$  for  $\mathbf{z} \in \mathbb{R}^n$  or  $\mathbb{C}^n$ .

In the following we consider the complex monic Mahler measure as a function

$$\begin{aligned} M_1 : \quad \mathbb{R}^{2n} &\rightarrow \mathbb{R} \\ (x_1, \dots, x_{2n}) &\mapsto M(X^n + (x_1 + ix_2)X^{n-1} + \dots + x_{2n-1} + ix_{2n}). \end{aligned}$$

We fix positive integers  $n, m, r, s$  with  $m = r + 2s$  and  $d_1, \dots, d_{r+s}$  such that  $d_i = 1$  for  $i = 1, \dots, r$  and  $d_i = 2$  for  $i = r+1, \dots, r+s$ . Moreover, let  $D = nm = n(r+2s)$ .

We define

$$(4.1) \quad Z = \left\{ (\mathbf{x}_1, \dots, \mathbf{x}_{r+s}, t) \in (\mathbb{R}^n)^r \times (\mathbb{R}^{2n})^s \times \mathbb{R} : \prod_{i=1}^{r+s} M_1(\mathbf{x}_i)^{d_i} \leq t \right\}.$$

Here  $\mathbf{x}_i \in \mathbb{R}^{d_i n}$  and  $M_1(\mathbf{x}_i)$  is the real or the complex monic Mahler measure respectively if  $i = 1, \dots, r$  or  $i = r+1, \dots, r+s$ .

We want to count lattice points in the fibers  $Z_t \subseteq \mathbb{R}^D$  using Theorem 3.2, therefore we need to show that  $Z$  is a semialgebraic set and that the fibers  $Z_t$  are bounded.

**Lemma 4.1.** *The set  $Z$  defined in (4.1) is semialgebraic.*

*Proof.* Recall the definition of  $Z$ . To each  $\mathbf{x}_i \in \mathbb{R}^{d_i n}$  corresponds a monic polynomial  $f_i$  of degree  $n$  with real (for  $i = 1, \dots, r$ ) or complex (for  $i = r+1, \dots, r+s$ ) coefficients. Let  $S$  be the set of points

$$(\mathbf{x}_1, \dots, \mathbf{x}_{r+s}, t, t_1, \dots, t_{r+s}, \boldsymbol{\alpha}^{(1)}, \boldsymbol{\beta}^{(1)}, \dots, \boldsymbol{\alpha}^{(r+s)}, \boldsymbol{\beta}^{(r+s)})$$

in  $\mathbb{R}^{n(r+2s)+1+r+s+2n(r+s)}$ , with  $\boldsymbol{\alpha}^{(i)}, \boldsymbol{\beta}^{(i)} \in \mathbb{R}^n$ , such that

- $\boldsymbol{\alpha}^{(i)}$  and  $\boldsymbol{\beta}^{(i)}$  are, respectively, the vectors of the real and the imaginary parts of the  $n$  roots of  $f_i$ , for every  $i = 1, \dots, r+s$ ;
- $\prod_{l=1}^n \max \left\{ 1, \left( \alpha_l^{(i)} \right)^2 + \left( \beta_l^{(i)} \right)^2 \right\} = t_i^2$  and  $t_i \geq 0$ , for every  $i = 1, \dots, r+s$ ;
- $\prod_{i=1}^{r+s} t_i^{d_i} \leq t$ .

It is clear that the set  $S$  is defined by polynomial equalities and inequalities. In fact, the first condition is enforced by the fact that the coordinates of  $\mathbf{x}_i$  are the images of  $\boldsymbol{\alpha}^{(i)}$  and  $\boldsymbol{\beta}^{(i)}$  under the appropriate symmetric functions, which are polynomials. The second and the third conditions are also clearly obtained by polynomial equalities and inequalities. Therefore,  $S$  is a semialgebraic set. The claim follows after noting that  $Z$  is nothing but the projection of  $S$  on the first  $n(r+2s)+1$  coordinates and applying the Tarski-Seidenberg principle (Theorem 3.1).  $\square$

Since  $M$  is a bounded distance function, there exists a positive real constant  $\gamma$  such that

$$\gamma|\mathbf{z}|_\infty \leq M(\mathbf{z}), \text{ for every } \mathbf{z} \in \mathbb{R}^{n+1} \text{ or } \mathbb{C}^{n+1},$$



where, if  $\mathbf{z} = (z_0, \dots, z_n) \in \mathbb{R}^{n+1}$  or  $\mathbb{C}^{n+1}$ ,  $|\mathbf{z}|_\infty = \max\{|z_0|, \dots, |z_n|\}$  is the usual max norm (see [4], Lemma 2, p. 108). Note that, since  $|(1, 0, \dots, 0)|_\infty = M(1, 0, \dots, 0) = 1$ ,  $\gamma$  must be less than or equal to 1. Clearly we have, for  $\mathbf{x} \in \mathbb{R}^n$

$$(4.2) \quad N(\mathbf{x}) := \gamma|(1, \mathbf{x})|_\infty \leq M_1(\mathbf{x})$$

in the real case and, for the complex case,

$$(4.3) \quad N(\mathbf{x}) := \gamma|(1, \mathbf{x})|_\infty \leq \gamma|(1, \mathbf{z})|_\infty \leq M_1(\mathbf{z}) = M_1(\mathbf{x}),$$

where  $\mathbf{x} = (x_1, \dots, x_{2n}) \in \mathbb{R}^{2n}$  and  $\mathbf{z} = (x_1 + ix_2, \dots, x_{2n-1} + ix_{2n})$ .

Recall that, by the definition, the monic Mahler measure function assumes values greater than or equal to 1, therefore, if  $(\mathbf{x}_1, \dots, \mathbf{x}_{r+s}) \in Z_t$  then  $M_1(\mathbf{x}_i)^{d_i} \leq t$  for every  $i$ . Thus,  $|\mathbf{x}_i|_\infty^{d_i} \leq \frac{t}{\gamma^{d_i}}$  and this means that  $Z_t$  is bounded for every  $t \in \mathbb{R}$ .

Now we can apply Theorem 3.2 to the family  $Z$ . If we set  $Z(T) = Z_T$ , we have

$$(4.4) \quad \left| |Z(T) \cap \Lambda| - \frac{\text{Vol}(Z(T))}{\det \Lambda} \right| \leq \sum_{j=0}^{D-1} C \frac{V_j(Z(T))}{\lambda_1 \cdots \lambda_j},$$

for every  $T \in \mathbb{R}$ , where  $\Lambda$  is a lattice in  $\mathbb{R}^D$  and  $C$  is a real constant independent of  $\Lambda$  and  $T$ .

## 5. PROOF OF THEOREM 2.1

We fix a number field  $k$  of degree  $m$  over  $\mathbb{Q}$ . The ring of integers  $\mathcal{O}_k$  of  $k$ , embedded into  $\mathbb{R}^{r+2s}$  via  $\sigma = (\sigma_1, \dots, \sigma_{r+s})$ , is a lattice of full rank. We embed  $(\mathcal{O}_k)^n$  in  $\mathbb{R}^D$  via  $\mathbf{a} \mapsto (\sigma_1(\mathbf{a}), \dots, \sigma_{r+s}(\mathbf{a}))$ , where the  $\sigma_i$  are extended to  $k^n$ . We want to count lattice points of  $\Lambda = (\mathcal{O}_k)^n$  inside  $Z(T)$ .

**Lemma 5.1.** *We have*

$$\det \Lambda = \left(2^{-s} \sqrt{|\Delta_k|}\right)^n,$$

and its first successive minimum is  $\lambda_1 \geq 1$ .

*Proof.* This is a special case of Lemma 5 of [10].  $\square$

Now we need to calculate the volume of  $Z(T)$ . We do something more general. Suppose we have  $r+s$  continuous functions  $f_i : \mathbb{R}^{n_i} \rightarrow [1, \infty)$ ,  $i = 1, \dots, r+s$  where  $1 \leq n_i \leq d_i n$  for every  $i$ . We define

$$(5.1) \quad Z_i(T) = \{\mathbf{x} \in \mathbb{R}^{n_i} : f_i(\mathbf{x}) \leq T\},$$

for every  $i = 1, \dots, r+s$ . Suppose that, for every  $i$ , there exists a polynomial  $p_i(X) \in \mathbb{R}[X]$  of degree  $n_i$  such that the volume of  $Z_i(T)$  is  $p_i(T)$  for every  $T \geq 1$ . Let  $C_i$  be the leading coefficient of  $p_i$ . Moreover, let

$$\tilde{Z}(T) = \left\{ (\mathbf{x}_1, \dots, \mathbf{x}_{r+s}) \in \mathbb{R}^{\sum n_i} : \prod_{i=1}^{r+s} f_i(\mathbf{x}_i)^{d_i} \leq T \right\}.$$

Note that, since  $f_i(\mathbf{x}_i) \geq 1$  for every  $i$ ,  $\tilde{Z}(T)$  is bounded for every  $T$ .

**Lemma 5.2.** *Let  $q = r+s-1$ . For every  $T \geq 1$  we have*

$$\text{Vol}(\tilde{Z}(T)) = \tilde{p}\left(T^{\frac{1}{2}}, \log T\right),$$

where  $\tilde{p}(X, Y) \in \mathbb{R}[X, Y]$ ,  $\deg_X \tilde{p} \leq 2n$ ,  $\deg_Y \tilde{p} \leq q$ . In the case  $n_i = d_i n$  for every  $i = 1, \dots, r+s$ , the coefficient of  $X^{2n} Y^q$  is  $\frac{n^q}{q!} \prod_{i=1}^{q+1} C_i$ . If  $n_i < d_i n$  for some  $i$  then the monomial  $X^{2n} Y^q$  does not appear in  $\tilde{p}$ .

*Proof.* We have

$$V(T) := \text{Vol} \left( \tilde{Z}(T) \right) = \int_{\tilde{Z}(T)} d\mathbf{x}_1 \dots d\mathbf{x}_{q+1}.$$

We proceed by induction on  $q$ . If  $q = 0$  there is nothing to prove. Suppose  $q > 0$  and let

$$\tilde{Z}^{(q)}(T) = \left\{ (\mathbf{x}_1, \dots, \mathbf{x}_q) \in \mathbb{R}^{n_1 + \dots + n_q} : \prod_{i=1}^q f_i(\mathbf{x}_i)^{d_i} \leq T \right\}.$$

Then

$$V(T) = \int_{Z_{q+1}} \left( T^{\frac{1}{d_{q+1}}} \right) \left( \int_{\tilde{Z}^{(q)}(T f_{q+1}(\mathbf{x}_{q+1})^{-d_{q+1}})} d\mathbf{x}_1 \dots d\mathbf{x}_q \right) d\mathbf{x}_{q+1}.$$

By the inductive hypothesis there exists  $\tilde{p}_q(X, Y) \in \mathbb{R}[X, Y]$  such that

$$V(T) = \int_{Z_{q+1}} \left( T^{\frac{1}{d_{q+1}}} \right) \tilde{p}_q \left( \left( \frac{T}{f_{q+1}(\mathbf{x}_{q+1})^{d_{q+1}}} \right)^{\frac{1}{2}}, \log \left( \frac{T}{f_{q+1}(\mathbf{x}_{q+1})^{d_{q+1}}} \right) \right) d\mathbf{x}_{q+1},$$

where  $\tilde{p}_q(X, Y) \in \mathbb{R}[X, Y]$ ,  $\deg_X \tilde{p}_q \leq 2n$ ,  $\deg_Y \tilde{p}_q \leq q-1$  and, if  $n_i = d_i n$  for every  $i = 1, \dots, q$ , the coefficient of  $X^{2n} Y^{q-1}$  is  $\frac{n^{q-1}}{(q-1)!} \prod_{i=1}^q C_i$ . If not, that monomial does not appear.

By  $\mathcal{L}^n$ , we indicate the Lebesgue measure on  $\mathbb{R}^n$ . Since  $f_{q+1}$  is a measurable function, we get

$$V(T) = \int_{\left[1, T^{\frac{1}{d_{q+1}}}\right]} \tilde{p}_q \left( \left( \frac{T}{X^{d_{q+1}}} \right)^{\frac{1}{2}}, \log \left( \frac{T}{X^{d_{q+1}}} \right) \right) d(\mathcal{L}^{n_{q+1}} \circ f_{q+1}^{-1})(X),$$

where we consider  $\mathcal{L}^{n_{q+1}} \circ f_{q+1}^{-1}$  as a measure on  $\left[1, T^{\frac{1}{d_{q+1}}}\right]$ . In particular for  $(u, v] \subseteq \left[1, T^{\frac{1}{d_{q+1}}}\right]$ ,

$$(\mathcal{L}^{n_{q+1}} \circ f_{q+1}^{-1})((u, v]) = p_{q+1}(v) - p_{q+1}(u),$$

and  $(\mathcal{L}^{n_{q+1}} \circ f_{q+1}^{-1})(\{1\}) = p_{q+1}(1)$ . Using 1.29 Theorem of [14], we get

$$\begin{aligned} V(T) &= \int_{\left[1, T^{\frac{1}{d_{q+1}}}\right]} \tilde{p}_q \left( \left( \frac{T}{X^{d_{q+1}}} \right)^{\frac{1}{2}}, \log \left( \frac{T}{X^{d_{q+1}}} \right) \right) p'_{q+1}(X) d\mathcal{L}^1(X) + \\ &\quad + \tilde{p}_q \left( T^{\frac{1}{2}}, \log T \right) p_{q+1}(1), \end{aligned}$$

where  $p'_{q+1}$  is the derivative of  $p_{q+1}$ .

For some integer  $c \geq 0$  we put  $L(X, c) = X^c$  in case  $c > 0$  and  $L(X, 0) = 1$ . Because of the linearity of the integral we are reduced to calculate

$$\begin{aligned} \mathcal{I}(a, b, c) &= \int_1^{T^{\frac{1}{d_{q+1}}}} X^a \left( \frac{T}{X^{d_{q+1}}} \right)^{\frac{b}{2}} L \left( \log \frac{T}{X^{d_{q+1}}}, c \right) dX = \\ &= T^{\frac{b}{2}} \int_1^{T^{\frac{1}{d_{q+1}}}} X^{a - \frac{b}{2} d_{q+1}} L \left( \log T - \log(X^{d_{q+1}}), c \right) dX, \end{aligned}$$

for some integers  $a, b, c$ , with  $0 \leq a \leq n_{q+1} - 1$ ,  $0 \leq b \leq 2n$  and  $0 \leq c \leq q - 1$ . Integrating by parts, one can see that  $\mathcal{I}(a, b, c)$  is a polynomial in  $T^{\frac{1}{2}}$  and  $\log T$ . In particular  $\mathcal{I}(a, b, c) = \widehat{p}(T^{\frac{1}{2}}, \log T)$ , where  $\widehat{p}(X, Y) \in \mathbb{R}[X, Y]$ , with  $\deg_X \widehat{p} \leq 2n$  and  $\deg_Y \widehat{p} \leq q$ . Note that in the case  $a = d_{q+1}n - 1$ ,  $b = 2n$  and  $c = q - 1$ , the coefficient of  $X^{2n}Y^q$  is  $\frac{1}{qd_{q+1}}$  and 0 for any other choice of  $a, b$  and  $c$ . Therefore, the monomial  $X^{2n}Y^q$  does not appear in  $\widehat{p}$  if either  $n_{q+1} < d_{q+1}n$  or  $X^{2n}Y^{q-1}$  does not appear in  $\widehat{p}_q$ , i.e., if  $n_i < d_i n$  for some  $i$ . To conclude, recall that, in the case  $n_i = d_i n$  for every  $i = 1, \dots, r + s$ ,  $p'_{q+1}$  has leading coefficient  $nd_{q+1}C_{q+1}$  and the coefficient of  $X^{2n}Y^{q-1}$  in  $\widehat{p}_q$  is  $\frac{n^{q-1}}{(q-1)!} \prod_{i=1}^q C_i$ .  $\square$

In [5], Chern and Vaaler calculated the volume of certain sets determined by the Mahler measure distance function. By (1.16) and (1.17) of [5], for every  $T \geq 1$  the volumes of the sets

$$(5.2) \quad \{(z_1, \dots, z_n) \in \mathbb{R}^n : M(1, z_1, \dots, z_n) \leq T\}$$

and

$$(5.3) \quad \{(z_1, \dots, z_n) \in \mathbb{C}^n : M(1, z_1, \dots, z_n)^2 \leq T\}$$

are, respectively, polynomials  $p_{\mathbb{R}}(T)$  and  $p_{\mathbb{C}}(T)$  of degree  $n$  and leading coefficients

$$C_{\mathbb{R},n} = 2^{n-M} \left( \prod_{l=1}^M \left( \frac{2l}{2l+1} \right)^{n-2l} \right) \frac{n^M}{M!},^1$$

with  $M = \lfloor \frac{n-1}{2} \rfloor$ , and

$$C_{\mathbb{C},n} = \pi^n \frac{n^n}{(n!)^2}.$$

Suppose  $q = 0$  and recall Lemma 5.1. We have

$$(5.4) \quad \frac{\text{Vol}(Z(T))}{\det \Lambda} = \frac{2^{sn}}{(\sqrt{|\Delta_k|})^n} C_{\mathbb{R},n}^r C_{\mathbb{C},n}^s T^n + \frac{P(T)}{(\sqrt{|\Delta_k|})^n},$$

for every  $T > 1$ , where  $P(X) \in \mathbb{R}[X]$  of degree  $n - 1$ .

**Corollary 5.3.** *Suppose  $q > 0$ . We have, for  $T > 1$ ,*

$$(5.5) \quad \frac{\text{Vol}(Z(T))}{\det \Lambda} = \frac{n^q 2^{sn}}{q! (\sqrt{|\Delta_k|})^n} C_{\mathbb{R},n}^r C_{\mathbb{C},n}^s T^n (\log T)^q + \frac{P(T^{\frac{1}{2}}, \log T)}{(\sqrt{|\Delta_k|})^n},$$

where  $P(X, Y) \in \mathbb{R}[X, Y]$ ,  $\deg_X P \leq 2n$ ,  $\deg_Y P \leq q$ , the coefficient of  $X^{2n}Y^q$  is 0.

*Proof.* By Lemma 5.2 and the result of Chern and Vaaler about the volumes of the sets defined in (5.2) and (5.3), the volume of  $Z(T)$  is  $p(T^{\frac{1}{2}}, \log T)$  where  $p(X, Y) \in \mathbb{R}[X, Y]$ ,  $\deg_X p \leq 2n$ ,  $\deg_Y p \leq q$  and the coefficient of  $X^{2n}Y^q$  is  $\frac{n^q}{q!} C_{\mathbb{R},n}^r C_{\mathbb{C},n}^s$ .  $\square$

---

<sup>1</sup>There is a misprint in (1.16) of [5],  $2^{-N}$  should read  $2^{-M}$ .

Therefore, recalling  $|\Delta_k|$  and  $\lambda_1, \dots, \lambda_D$  are greater than or equal to 1, by (5.4) and Corollary 5.3, (4.4) becomes

$$(5.6) \quad \left| |Z(T) \cap \Lambda| - \frac{n^q 2^{sn}}{q! \left(\sqrt{|\Delta_k|}\right)^n} C_{\mathbb{R},n}^r C_{\mathbb{C},n}^s T^n (\log T)^q \right| \leq \sum_{j=0}^{D-1} CV_j(Z(T)) + Q(T),$$

for every  $T > 1$ , where  $Q(T)$  is the function of  $T$  obtained from the polynomial  $P$  of (5.4) or (5.5) substituting the coefficients with their absolute values. Note that  $Q$  depends only on  $m$  and  $n$ .

Now we want to find a bound for  $V_j(Z(T))$ . Recall that in (4.2) and (4.3) we have defined a function  $N(\mathbf{x}) = \gamma|(1, \mathbf{x})|_\infty$  such that  $N(\mathbf{x}) \leq M_1(\mathbf{x})$ . Let

$$Z'(T) = \left\{ (\mathbf{x}_1, \dots, \mathbf{x}_{r+s}) \in \mathbb{R}^D : \prod_{i=1}^{r+s} N(\mathbf{x}_i)^{d_i} \leq T \right\}.$$

Each  $(\mathbf{x}_1, \dots, \mathbf{x}_{r+s})$  with  $\prod_{i=1}^{r+s} M_1(\mathbf{x}_i)^{d_i} \leq T$  satisfies  $\prod_{i=1}^{r+s} N(\mathbf{x}_i)^{d_i} \leq T$ . Therefore, we have  $Z(T) \subseteq Z'(T)$  and  $V_j(Z(T)) \leq V_j(Z'(T))$ .

Suppose  $q = 0$ . This means that  $k$  is either  $\mathbb{Q}$  ( $m = 1$ ) or an imaginary quadratic field ( $m = 2$ ). In any case any projection of  $Z'(T)$  to a  $j$ -dimensional coordinate subspace has volume  $\left(\frac{2}{\gamma}\right)^j T^{\frac{j}{m}}$  if  $T \geq \gamma^m$ , for every  $j = 1, \dots, D-1$ . Therefore we obtain

$$(5.7) \quad V_j(Z(T)) \leq V_j(Z'(T)) \leq ET^{n-\frac{1}{m}},$$

for some real constant  $E$  depending only on  $n$  and  $m$ . This holds for every  $T > 1$  since  $\gamma \leq 1$ .

Now suppose  $q > 0$ .

**Lemma 5.4.** *For every  $j = 1, \dots, D-1$ , there exists a polynomial  $P_j(X, Y) \in \mathbb{R}[X, Y]$  whose coefficients depend only on  $m$  and  $n$ , with  $\deg_X P_j \leq 2n$ ,  $\deg_Y P_j \leq q$ , and the coefficient of  $X^{2n}Y^q$  is 0, such that, for every  $T > 1$ , we have*

$$V_j(Z'(T)) = P_j\left(T^{\frac{1}{2}}, \log T\right).$$

*Proof.* By definition, the projection of  $Z'(T)$  on a  $j$ -dimensional coordinate subspace is just the intersection of  $Z'(T)$  with such subspace. To each such subspace  $\Sigma$  we can associate integers  $n_1, \dots, n_{r+s}$  with  $0 \leq n_i \leq d_i n$  such that  $\Sigma$  is defined by setting  $d_i n - n_i$  coordinates of each  $\mathbf{x}_i$  to 0. Therefore we are in the situation of Lemma 5.2 because, after dividing by  $\gamma$ , we have, for every  $i$  such that  $n_i > 0$ , a continuous function  $f_i : \mathbb{R}^{n_i} \rightarrow [1, \infty)$ , with  $\sum n_i = j$ . This gives rise to sets of the form (5.1), whose volumes are  $2^{n_i} T^{n_i}$ . Since  $j < D$ , not all  $n_i$  can be equal to  $d_i n$ . Therefore, by Lemma 5.2, the volume of any such projection equals a polynomial with the desired property and we have the claim.  $\square$

Recall the definition of  $\mathcal{M}^k(e, \mathcal{H})$  that was given in Section 2. Clearly  $|\mathcal{M}^k(e, \mathcal{H})|$  is the number of  $\mathbf{a} \in \mathcal{O}_k^e$  with  $\prod_{i=1}^{r+s} M_1(\sigma_i(\mathbf{a}))^{d_i} \leq \mathcal{H}^m$ , i.e.,  $|Z(\mathcal{H}^m) \cap \mathcal{O}_k^e|$ .

By (5.6), (5.7) and Lemma 5.4 we have, for every  $\mathcal{H} > 1$ ,

$$\left| |\mathcal{M}^k(e, \mathcal{H})| - \frac{e^q m^q 2^{se}}{q! \left(\sqrt{|\Delta_k|}\right)^e} C_{\mathbb{R},e}^r C_{\mathbb{C},e}^s \mathcal{H}^{me} (\log \mathcal{H})^q \right| \leq E(\mathcal{H}),$$

with

$$E(\mathcal{H}) = \begin{cases} \sum_{i=0}^{2me} \sum_{j=0}^q E_{i,j} \mathcal{H}^{\frac{i}{2}} (\log \mathcal{H})^j, & \text{if } q \geq 1, \\ \sum_{i=0}^{me-1} E_i \mathcal{H}^i, & \text{if } q = 0, \end{cases}$$

where  $E_{2me,q} = 0$  and all the coefficients depend on  $m$  and  $e$ .

Finally, it is clear that for every  $\mathcal{H}_0 > 1$  one can find a  $D_0$  such that, for every  $\mathcal{H} \geq \mathcal{H}_0$ ,

$$E(\mathcal{H}) \leq \begin{cases} D_0 \mathcal{H}^{me} (\log \mathcal{H})^{q-1}, & \text{if } q \geq 1, \\ D_0 \mathcal{H}^{me-1}, & \text{if } q = 0, \end{cases}$$

and we derive the claim of Theorem 2.1.

#### ACKNOWLEDGMENTS

The author would like to thank Martin Widmer for sharing his ideas, for his constant encouragement and for several suggestions that improved this article and Robert Tichy and Jeff Vaaler for many useful discussions.

#### REFERENCES

1. F. Barroero and M. Widmer, *Counting lattice points and o-minimal structures*, submitted.
2. E. Bierstone and P. D. Milman, *Semianalytic and subanalytic sets*, Inst. Hautes Études Sci. Publ. Math. (1988), no. 67, 5–42.
3. E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.
4. J.W.S. Cassels, *An introduction to the geometry of numbers*, Grundlehren der mathematischen Wissenschaften, Springer-Verlag, 1971.
5. S. Chern and J. D. Vaaler, *The distribution of values of Mahler's measure*, J. reine angew. Math. **540** (2001), 1–47.
6. H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179–183.
7. X. Gao, *On Northcott's theorem*, Ph.D. Thesis, University of Colorado (1995).
8. S. Lang, *Fundamentals of Diophantine geometry*, Springer-Verlag, New York, 1983.
9. K. Mahler, *On the zeros of the derivative of a polynomial*, Proc. Roy. Soc. Ser. A **264** (1961), 145–154.
10. D. Masser and J. D. Vaaler, *Counting algebraic numbers with large height. II*, Trans. Amer. Math. Soc. **359** (2004), no. 1, 427–445.
11. J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999.
12. D. G. Northcott, *An inequality in the theory of arithmetic on algebraic varieties*, Proc. Cambridge Philos. Soc. **45** (1949), 502–509.
13. J. Pila and A. J. Wilkie, *The rational points of a definable set*, Duke Math. J. **133** (2006), no. 3, 591–616.
14. W. Rudin, *Real and complex analysis*, McGraw-Hill Book Co., New York, 1966.
15. S. H. Schanuel, *Heights in number fields*, Bull. Soc. Math. France **107** (1979), no. 4, 433–449.
16. W. M. Schmidt, *Northcott's theorem on heights. I. A general estimate*, Monatsh. Math. **115** (1993), no. 1-2, 169–181.
17. ———, *Northcott's theorem on heights II. The quadratic case*, Acta Arith. **LXX.4** (1995), 343–375.
18. M. Widmer, *Integral points of fixed degree and bounded height*, preprint.
19. ———, *Counting points of fixed degree and bounded height*, Acta Arith. **140** (2009), no. 2, 145–168.

*E-mail address:* barroero@math.tugraz.at

INSTITUT FÜR MATHEMATIK A, TECHNISCHE UNIVERSITÄT GRAZ, STEYRERGASSE 30, A-8010 GRAZ, AUSTRIA